Unix系统安全必读（2） PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/144/2021_2022_Unix_E7_B3_BB_E7_BB_9F_c103_144164.htm (3)设备文件 UNIX系统与边在本系统上的各种设备之间的通讯,通过特别文件来实现就程序而言,磁盘是文件,MODEM是文件,甚至内存也是文件.所有连接到系统上的设备都在/dev目录中有一个文件与其对应.当在这些文件上执行I/O操作时,由UNIX系统将I/O操作转换成实际设备的动作.例如,文件/dev/mem是系统的内存,如果cat这个文件,实际上是在终端显示系统的内存.为了安全起见,这个文件对普通用户是不可读的.因为在任一给定时间,内存区可能含有用户登录口令或运行程序的口令,某部分文件的编辑缓冲区,缓冲区可能含有用ed -x命令解密后的文本,以及用户不愿让其他人存取的种种信息.在/dev中的文件通常称为设备文件,用ls /dev命令可以看看系统中的一些设备: acuo 呼叫自动拨号器 console 系统控制台 dsknn 块方式操作磁盘分区 kmem 核心内存 mem 内存 lp 打印机 mto 块方式操作磁带 rdsknn 流方式操作的磁盘分区 rmto 流方式操作的磁带 swap 交换区 sysc on 系统终端 ttynn 终端口 x25 网络端口 等等 (4)/etc/mknod命令 用于建立设备文件.只有root能使用这个命令建立设备文件.其参数是文件名,字母c或b分别代表字符特别文件或块特别文件,主设备号,次设备号.块特别文件是像磁带,磁盘这样一些以块为单位存取数据的设备.字符特别文件是如像终端,打印机,MODEM,或者其它任何与系统通讯时,一次传输一个字符的设备,包括模仿对磁盘进行字符方式存取的磁盘驱动器.主设备号指定了系统子程序(设备驱动程序),当在设备上执行I/O时,系统将调用

这个驱动程序.调用设备驱动程序时,次设备号将传递给该驱动程序(次设备规定具体的磁盘驱动器,带驱动器,信号线编号,或磁盘分区).每种类型的设备一般都有自己的设备驱动程序. 文件系统将主设备号和次设备号存放在i节点中的磁盘地址表内,所以没有磁盘空间分配给设备文件(除i节点本身占用的磁盘区外).当程序试图在设备文件上执行I/O操作时,系统识别出该文件是一个特别文件,并调用由主设备号指定的设备驱动程序,次设备号作为调用设备驱动程序的参数. (5)安全考虑 将设备处理成文件,使得UNIX程序独立于设备,即程序不必一定要了解正使用的设备的任何特性,存取设备也不需要记录长度,块大小,传输速度,网络协议等这样一些信息,所有烦人的细节由设备驱动程序去关心考虑,要存取设备,程序只须打开设备文件,然后作为普通的UNIX文件来使用.从安全的观点来看这样处理很好,因为任何设备上进行的I/O操作只经过了少量的渠道(即设备文件).用户不能直接地存取设备.所以如果正确地设置了磁盘分区的存取许可,用户就只能通过UNIX文件系统存取磁盘.文件系统有内部安全机制(文件许可).不幸的是,如果磁盘分区设备得不正确,任何用户都能够写一个程序读磁盘分区中的每个文件,作法很简单:读一i节点,然后以磁盘地址表中块号出现的顺序,依次读这些块号指出的存有文件内容的块.故除了root以外,决不要使盘分区对任何人可写.因为所有者,文件存取许可方式这样一些信息存放于i节点中,任何人只要具有已安装分区的写许可,就能设置任何文件的SUID许可,而不管文件的所有者是谁,也不必用chmod()命令,还可避过系统建立的安全检查. 以上所述对内存文件mem,kmem和对换文件swap也是一样的.这些文件含有用户信息,一个"耐心"的程序可以将用户

信息提取出来.要避免磁盘分区(以及其它设备)可读可写,应当在建立设备文件前先用umask命令设置文件建立屏蔽值. 一般情况下,UNIX系统上的终端口对任何人都是可写的,从而使用户可以用write命令发送信息.虽然write命令易引起安全方面的问题,但大多数用户觉得用write得到其他用户的信息很方便,所以系统将终端设备的存取许可设置成对所有用户可写. /dev目录应当是755存取许可方式,且属root所有. 不允许除root外的任何用户读或写盘分区的原则有一例外,即一些程序(通常是数据库系统)要求对磁盘分区直接存取,解决这个问题的经验的盘分区应当由这种程序专用(不安装文件系统),而且应当告知使用这种程序的用户,文件安全保护将由程序自己而不是UNIX文件系统完成. (6)find命令 find命令用于搜索目录树,并对目录树上的所有文件执行某种操作,参数是目录名表(指出从哪些起点开始搜索),还可给出一个或多个选项,规定对每个文件执行什么操作. find . -print 将列出当前工作目录下的目录树的每一个文件.find / -user bob -print 将列出在系统中可找到的属于bob用户的所有文件. find /usr/bob -perm 666 -print 将列出/usr/bob目录树下所有存取许可为666的文件.若将666改为-666则将列出所有具有包含了666在内的存取许可方式的文件(如777). find /usr/bob -type b -print 将列出/usr/bob目录树下所有块特别文件(c为字符特别文件). find / -user root -perm -4000 -exec ls -l {} \. 是一个较复杂一点的命令,-exec COMMAND \.允许对所找到的每个文件运行指定的命令COMMAND.若COMMAND中含有{},则{}将由find所找到的文件名替换.COMMAND必须以\.结束. 以上举例介绍find的用法,各选项可组合使用以达到更强的功能. (7)secure程序 系统管理员应当做一个程序以定期检查系

统中的各个系统文件,包括检查设备文件和SUID,SGID程序,尤其要注意检查SUID,SGID程序,检查/etc/passwd和/etc/group文件,寻找久未登录的户头和校验各重要文件是否被修改.(源程序清单将在今后发表) 